

FILED

ORIGINAL

## UNITED STATES DISTRICT COURT

2015 JAN 22 PM 2:28

for the  
CLERK U.S. DISTRICT COURT  
CENTRAL District of California  
SANTA ANAIn the Matter of the Search of \_\_\_\_\_  
(Briefly describe the property to be searched  
or identify the person by name and address)3 Laurelwood Street,  
Aliso Viejo, California 92656

Case No.

SA 15-006M

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California  
(identify the person or describe the property to be searched and give its location):

See Attachment A-1

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property. Such affidavit(s) or testimony are incorporated herein by reference and attached hereto.

**YOU ARE COMMANDED** to execute this warrant on or before 14 days from the date of its issuance  
(not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

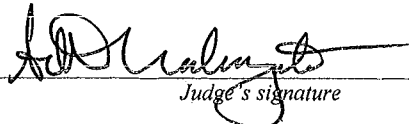
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for \_\_\_\_\_ days (not to exceed 30).☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued:

January 9, 2015 at 12:18p.

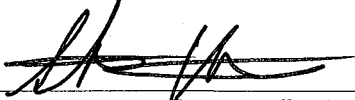
  
Judge's signatureCity and state: Santa Ana, California

ARTHUR NAKAZATO, U.S. Magistrate Judge

Printed name and title



AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
SA15 - 006M	01/21/2015 7:00 AM	QAYED SHAREEF
Inventory made in the presence of:		
QAYED SHAREEF		
<p>Inventory of the property taken and name of any person(s) seized:</p> <p>[Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]</p> <ul style="list-style-type: none"> <li>- BLUE SWEATSHIRT WITH THE LETTERS "GAP" ON THE FRONT.</li> <li>- 1 SUPPLEMENTAL TAX BILL DOCUMENT WITH THE SUBJECT NAME AND ADDRESS ON IT.</li> <li>- 1 HANDHELD MASSAGER, LIGHT BLUE IN COLOR.</li> <li>- 1 APPLE IPHONE, SERIAL NUMBER 354452061022</li> <li>- 1 APPLE MAC BOOK PRO COMPUTER S/N: C02FTGG4DH2G</li> <li>- 1 APPLE IMAC COMPUTER S/N: W8807935X86</li> <li>- 1 APPLE MAC BOOK AIR COMPUTER S/N: C02FH264DDQW</li> <li>- 1 APPLE IPHONE S/N: 890002861596862</li> <li>- 1 APPLE MAC BOOK AIR COMPUTER S/N: C02NK00EG5RK</li> </ul>		
Certification (by officer present during the execution of the warrant)		
<p>I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.</p>		
Date: 1/22/2015	 Executing officer's signature	
SCOTT WITTMIER, SPECIAL AGENT Printed name and title		

ATTACHMENT A1

PREMISES TO BE SEARCHED

The SUBJECT RESIDENCE is the property located at 3 Laurelwood Street, Aliso Viejo, California 92656, which is further described as follows: a single-family, two story residence that appears to be tan in color with white trim around the windows. The residence has a two-car garage with a white door. There are white steps with a white railing leading to the front porch. There is a black number "3" with a white background to the left of the garage door.

Instrumentality Protocol

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography), 2252A(a)(5)(B) (possession of child pornography), and 2251(a) (production of child pornography), namely:

- a. Blue sweatshirt with the letters "GA" printed on it;
- b. Glass dildos or other glass sex toys;
- c. Any digital devices used to facilitate the above-listed violations and forensic copies thereof.
- d. Records, documents, programs, applications, or materials containing child pornography, as defined in 18 U.S.C. § 2256.
- e. Any records, documents, programs, applications or materials pertaining to the possession, receipt, distribution and/or reproduction of child pornography, as defined in 18 U.S.C. § 2256.
- f. Any records, documents, programs, applications or materials identifying persons transmitting or receiving, through interstate commerce, including by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

g. Any records, documents, programs, applications or materials referring to the production, receipt, shipment, order, request, trade, purchase or transaction of any kind involving the transmission through interstate commerce, including by computer, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

h. Any records, documents, programs, applications or materials referring to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce, including by computer, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

i. Any records, documents, programs, applications or materials that list names and addresses of any minor visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

j. Any records, documents, programs, applications or materials that show the offer to transmit through interstate commerce any depictions of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

k. Any and all materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict

Instrumentality Protocol

minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings. "Child erotica" may also include, in this context, sex aids and/or toys.

1. Electronically stored communications or messages reflecting computer on-line chat sessions or e-mail messages with a minor that are sexually explicit in nature, as defined in 18 U.S.C. § 2256.

m. Any documents, records, programs, or applications that identify the residents of the SUBJECT PREMISES.

n. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

Instrumentality Protocol

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

4. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.



5. In order to determine whether non digital video media, such as analog VHS or Beta tapes, contain material responsive to the search warrant, law enforcement personnel executing the search warrant will view them onsite provided the equipment necessary to view the tapes is present and provided there is not more than three hours' worth of viewing material; otherwise, it will be seized and searched offsite as is practicable but not to exceed 60 days from the date of execution of this warrant. If additional time is needed, the government may seek an extension of this time period from the Court within the original 60-day period from the date of execution of the warrant. If the search determines that the non-digital media is not itself an item to be seized and does not contain any data falling within the list of the items to be seized pursuant to this warrant, the government will return it.

## **II. SEARCH PROCEDURE FOR DIGITAL DEVICES**

6. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team

Instrumentality Protocol

shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The team searching the digital device may use sophisticated hashing tools, such as tools identifying child pornography. The tools most commonly used to identify child pornography are "En case" and "FTK" (Forensic Tool Kit).

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

g. The government may retain a digital device itself, and/or entire forensic copies of it, until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be

Instrumentality Protocol

an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device and/or forensic copies of it (or while an application for such an order is pending). Otherwise, the government must return the device and delete or destroy all forensic copies thereof.

h. Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

7. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

- a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;
- b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;
- c. Any magnetic, electronic, or optical storage device capable of storing digital data;
- d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.